

Connecting**Ontario**

File Encryption and Transfer Guideline

Version: 2

Document ID: 2551

Document Owner: Security Services

Copyright Notice

Copyright © 2016, eHealth Ontario

All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of eHealth Ontario. The information contained in this document is proprietary to eHealth Ontario and may not be used or disclosed except as expressly authorized in writing by eHealth Ontario.

Trademarks

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Introduction

eHealth Ontario policies require that adequate safeguards be applied every time a sensitive document or file is stored or transferred through communications channels that are not considered safe and secure such as regular internet email, CDs, DVDs, USB sticks and/or flash memory card.

This document provides instructions on how to apply a strong level of protection to sensitive files and reports, using WinZip, a commercially available application that can be used both to reduce the size of a document and to apply strong protection.

It is important to keep in mind that the encryption tool described in this document is a password based cryptosystem. The protection of file encryption can be broken if the associated password is compromised. Therefore, it is required that the password protection guidelines described in the “password sharing” section be applied by anyone who uses the tool and is involved in the file encryption process.

Authorized Uses

This process can be used whenever there is an occasional need for any sensitive information to be transferred over email consistent with regular business processes, including documents that contain personal information and/or personal health information.

If sending sensitive information over non-secure email is an ongoing business process, considerations should be made to automate the process and use an enterprise mechanism to securely transfer the information.

eHealth Ontario’s limit on email attachments is 10 MB per email.

For further assistance please contact the eHealth Ontario Service Desk at 1-866-250-1554.

File Encryption using WinZip

*eHealth Ontario uses the **WinZip 16.0** standard version within the agency to encrypt and zip files. If your computer does not have WinZip installed, you may contact your site help desk for assistance or use Microsoft Word or Excel for encryption. The following describes the steps for using WinZip, Microsoft Word and Excel.*

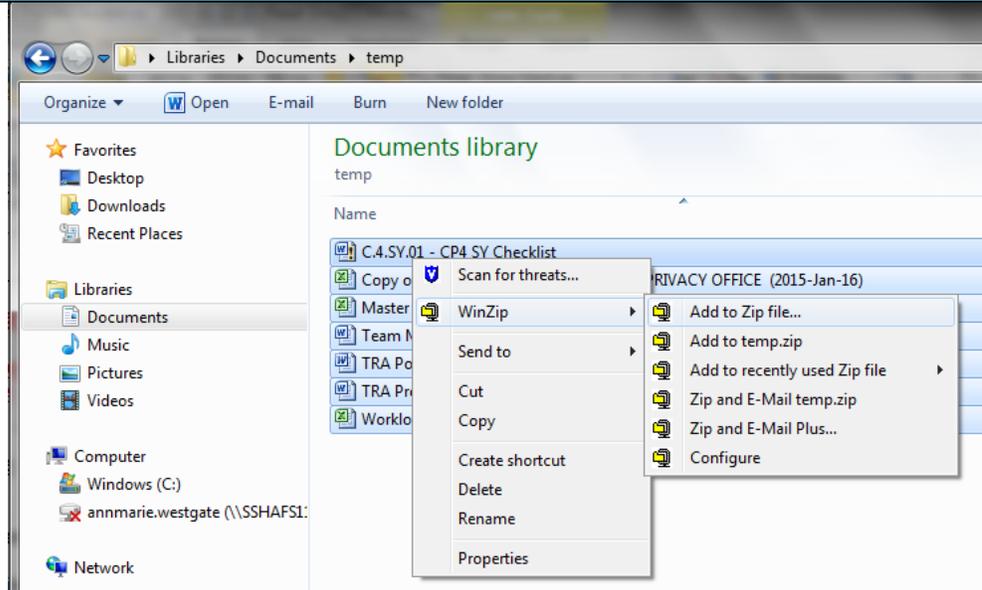
Encrypting Files using WinZip

Step 1. Create Archive

Open the file location.

Navigate to the folder where the files are. Using the mouse, select the files you wish to zip. On the dialogue box that opens float your mouse over WinZip and choose to **Add to Zip file...**

Assign the file name you wish to use.



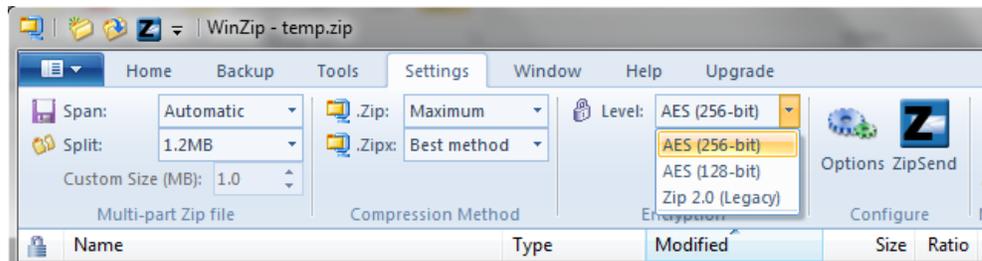
Step 1. Add files to an archive

Step 2. Open the Archive:

Double click on the zip file to open the archive.

Step 3. Choose a stronger encryption mechanism

Use AES 256-bit encryption. In the **Settings** tab, ensure the encryption level selected is **AES (256-bit)**.

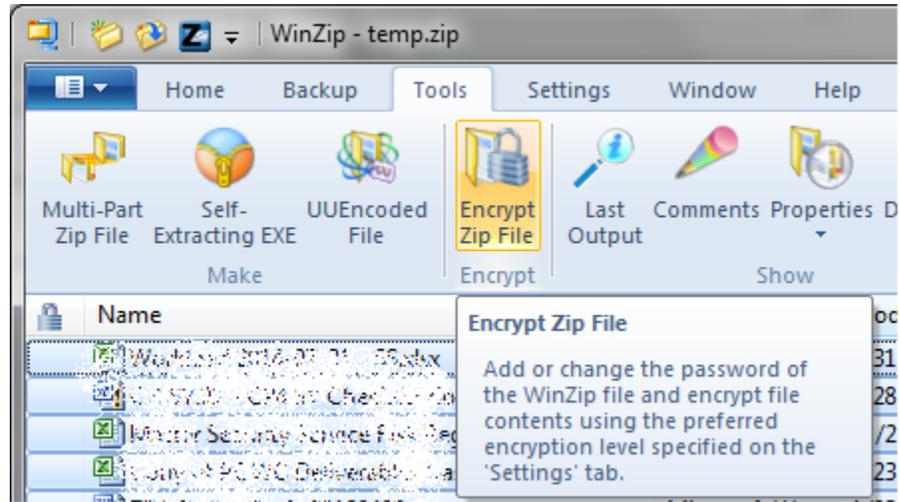


Step 3 Choose an encryption mechanism

Encrypting Files using WinZip

Step 4. Encrypt the entire file

From the Tools menu, click on **Encrypt Zip File**



Step 4. Encrypt the Zip File

Step 5. Create a strong password

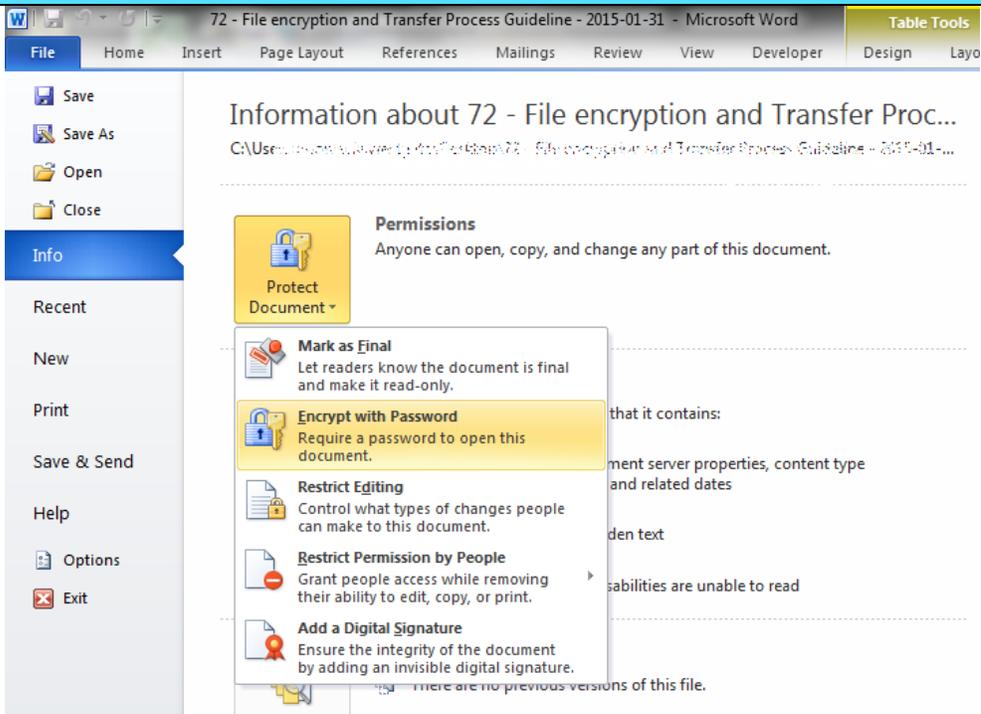
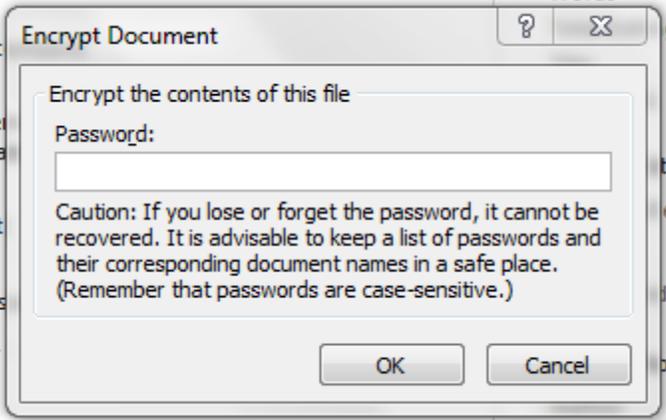
Enter a password and then confirm it.

See Section 0 below for how to create a strong password.

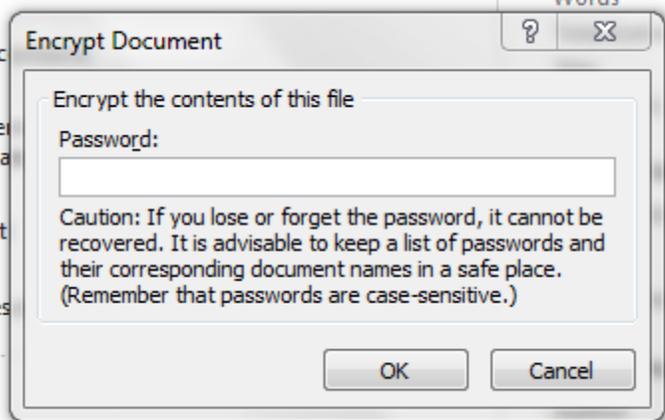


Fig.4 Create a strong password

Encrypting a Microsoft Word Document

Encrypting Files using Microsoft Word 2010	
<p>Step 1. Protect Document Open the document.</p> <p>Click on the File tab, and click on Info.</p> <p>Select Protect Document.</p> <p>In the pull down menu, choose Encrypt with Password.</p>	 <p style="text-align: center;">Step 1. Choose to Protect Document</p>
<p>Step 2: Enter a password and then confirm it.</p> <p>See Section o below for how to create a strong password.</p>	 <p style="text-align: center;">Step 2 Enter and confirm your password</p>

Encrypting a Microsoft Excel Document

Encrypting Files using Microsoft Excel 2010	
<p>Step 1. Protect Document Open the document.</p> <p>Click on the File tab, and click on Info.</p> <p>Select Protect Document.</p> <p>In the pull down menu, choose Encrypt with Password.</p>	 <p>The screenshot shows the Microsoft Excel 2010 interface. The 'File' tab is selected, and the 'Info' section is expanded. The 'Protect Workbook' option is highlighted in yellow, and the 'Encrypt with Password' option is also highlighted in yellow. The 'Permissions' section is visible, showing that 'Anyone can open, copy, and change any part of the workbook'. The 'Mark as Final' and 'Protect Current Sheet' options are also visible.</p> <p>Step 1. Choose to Protect Document</p>
<p>Step 2: Enter a password and then confirm it.</p> <p>See Section 0 below for how to create a strong password.</p>	 <p>The screenshot shows the 'Encrypt Document' dialog box. The title bar reads 'Encrypt Document'. The main text says 'Encrypt the contents of this file'. There is a 'Password:' label followed by a text input field. Below the input field, there is a caution message: 'Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place. (Remember that passwords are case-sensitive.)'. At the bottom, there are 'OK' and 'Cancel' buttons.</p> <p>Step 2 Enter and confirm your password</p>

Password Creation

It is important to create a strong password with which to protect encrypted files.

- Create and use a different password for each different encrypted document.
- Use 8 characters or more.
- Passwords must contain characters from three of the following four categories: uppercase characters (A-Z); lowercase characters (a-z); numeric (0-9); and special characters (e.g.!, \$, #, _, ~, %, ^).
- Example of a bad password is *1234Password!*
- Example of a good password is *iT_iS_A_warM_daY22*

Once the file has been encrypted, the password must be communicated to the file recipient by using an “out of band” method (e.g. if emailing document, send password by phone, fax or mail). In other words, the password should not be sent at the same time using the same method as the encrypted file.

The file must be encrypted and password protected before the sender transfers it to the requester as an attachment to an email message.

WinZip, described in this document, supports symmetric encryption. This requires the exchange of a shared secret (password in this case). In other words, the sender of the encrypted file must communicate the password to the intended recipient of the file. WinZip does not provide a method for retrieving files from an encrypted archive if a password is forgotten. The password creation and sharing therefore requires special attention.

Password Sharing

Passwords must be securely shared when being sent to eHealth Ontario from a HIC.

The procedures are as follows:

- Determine the authorized recipient of the information
- Make the encrypted file available to the recipient using agreed process (e.g. SFTP, email)
- The requestor calls the sender by phone
- The sender verbally verifies the recipient’s identity:
 - name
 - title, business unit, organization
 - name of received / retrieved encrypted file
- Verbally provide the verified recipient with the password to open the encrypted file
- Request and obtain verbal confirmation that the recipient has been able to extract the file(s)
- The sender securely destroys the written copy (if any) of the password and deletes any copies of the file from any local or network drives

Password Recovery

WinZip does not provide a mechanism for password recovery. Therefore, in the case of long term storage of encrypted files, a method of password recovery must be in place to access these files (e.g. if an employee leaves and their files need to be accessed).

An example of a password recovery method is storing the password in a sealed envelope which can only be accessed by upper management and will only be accessed for password recovery purposes.

File deletion

Once the encrypted file is no longer needed, it must be deleted by both the sender and the requester of the file.